What Is Claimed Is:

1. A method of declaring an incident in an enterprise comprising:

providing a number of alert indications containing information concerning an incident related to the enterprise; and either

comparing one or more of the alert indications to a set of rules, and if a match occurs between the set of rules, and the alert indication, declaring an incident based on the match, or

comparing one or more of the alert indications to a decision table containing a number of defined alert events; remembering each alert indication that matches one of the defined alert events, comparing the remembered alert indication to correlation data in the decision table, and if a match occurs between the remembered alert indication and the correlation data, declaring an incident based on the match; or

if no match occurs between the alert indication and the correlation data or the rules set, declare an incident if the alert indication meets a defined default threshold value.

2. The method of claim 1, wherein the defined default threshold value is a level of severity in the alert indication.

3. The method of claim 1, further comprising displaying an incident ticket for each incident declared, the incident ticket

including a description of the incident, a conclusion based on incident description, any actions responsive to the conclusion, one or more incident tracking rules which identify one or more further alert indications for association with the incident ticket, and a detail of the alert indications associated with the incident.

4. The method of claim 1, further comprising the step of tracking further alert indications once an incident ticket is declared and associating the further alert indications with the incident ticket based on one or more incident tracking rules.

5. The method of claim 4, wherein the associating step is performed only if the further alert indications pass a threshold value or table lookup from a user-editable table which lists enterprise policy attributes associated with particular alert codes, categories, or threat characterizations.

6. The method of claim 4, further comprising updating the incident tracking rules based on one or more further alert indications.

7. The method of claim 1, wherein the alert indications include information having a common format.

8. The method of claim 1, wherein the enterprise is a network with a number of network devices that supply the alert indications for incident declaration.

9. The method of claim 1, wherein the default defined value derives from a set of rules defining default conditions for declaring an incident.

10. A system for declaring an incident in an enterprise comprising:

a) a decision table containing a number of defined alert events, and a set of correlation data that identifies patterns in alert indications inputted to the decision table, the decision table remembering inputted alert indications matching defined alert events, and declaring an incident if a match occurs between remembered alert indications and the correlated data;

a set of rules containing a number of query statements, wherein a match between at least one of the rules and the inputted alert indications result in an incident declaration; and

a set of default standards specifying a minimum value to declare an incident should a match not occur with the decision tables or set of rules.

11. The system of claim 10, further comprising a display of the incident as an incident ticket, the incident ticket including a description of the incident, a conclusion based on incident

description, any actions responsive to the conclusion, one or more incident tracking rules which identify one or more further alert indications for association with the incident ticket, a detail of the alert indications associated with the incident, followed by a listing of "raw events" that, if requested by the user, contains information that has been left in the native or vendor-specific format of the original sensor that produced the event.

12. The system of claim 10, further comprising an alert processing system that tracks inputted alert indications, filters out inputted alert indications that do not meet a threshold value, compares the inputted information to a tracking rule to determine whether the inputted information should be associated with a declared incident.

13. The system of claim 10, further comprising a database for storing at least the declared incidents.

14. The system of claim 12, further comprising a database for storing at least the declared incidents and alert indications passing the threshold value.

15. The system of claim 13, further comprising a web server, linking the system to one or more users via a global network.

16. The system of claim 10, further comprising means for displaying the declared incident.

17. The system of claim 10, wherein the rules are a combination of default rules and customized rules.

18. The system of claim 10, wherein the enterprise is a network and the inputted information is supplied by a number of network devices.

19. The system of claim 12, further comprising an alert processing system that tracks inputted alert indications, filters out inputted alert indications that do not meet a threshold value, compares the inputted information to a tracking rule to determine whether the inputted information should be associated with a declared incident.

20. The system of claim 19, wherein the enterprise is a network, and the inputted information is supplied by a number of network devices.

21. The method of claim 3, comprising updating the incident ticket based an updated tracking rule such that the alert indications, conclusions and description reflect the updated tracking rule.

22. The method of claim 21, wherein the tracking rule is updated using human input based on observations of reported incidents.